E:\TRA-v/KMS Project /pR

Issue of Smart Card based Driving Licences, Formation of State and Regional Key Management Authorities and Appointment of Nodal Officer.

GOVERNMENT OF MAHARASTRA

HOME DEPART MENT

Governament Resolution no : MVD-1205/C.R.134/ TRA-4, Mantralay, Mumbai - 400032, Dated - July 1, 2005.

Read : 1) Transport Commissioner's, Maharashtra State, Mumbai, lettter no : TC/Br.11/Computer/140/2005/Outward No- 2448, Dt. 21 st Feb., 2005.

2) Government of India's (Ministry of Communications and Information Technology, Department of Information Technology, National Information Centre, A Block, CGO Complex, Lodhi Road, New Delhi-110003.) D.O. letter No.NIC/TD(SKR)/2005/14, dated 11/01/2005.

Government Resolution : The Ministry of Road Transport and Highways in the Govt. of India has decided to implement the project of providing Smart Card based Driving Licences.

1. In order to develop the smart card based technology usage in Motor Vehicle Departments the Govt. of India has entered into a MoU with National Informatics Centre, New Delhi. While using the Smart Card based technology it requires Security measures and authentication of information stored in the smart card. For this purpose "Key Management System" is to be applied. This system is based on three tiers, Which are as follows-

(1) Central Key Generation Authority (CKGA)

(2) State Key Management Authority (SKMA)

(3) Regional Key Management Authority (RKMA)

(which includes Sub-Regional Key Management Authority)

...2...

2. "National Informatics Centre" in association with "Price Waterhouse Coopers" has developed a SKI Practice Statement (Key Management Proceedures) which has been approved by the Ministry of Road Tranport and Highways. Out of these above mentioned tiers in the first phase, the first Tier namely CKGA has been established at NIC-New Delhi. Now, in the second phase, SKMA is to be established in the State Motor Vehicle Dept. and in the third phase, RKMA is to be established in the offices of Regional Transport Offices & Sub RKMA in the offices of Deputy Regional Transport Offices.

3. Accordingly the Govt. of India vide its letter dated 11-01-2005 has informed to establish SKMA and RKMA and appoint the Nodal Officers. In this background, the Commissioner of Transport, Maharashtra State, Mumbai vide its letter dated 21-02-2005 has requested to appoint Deputy Transport Commissioner (Computer), Office of the Commissioner of Transport, Maharashtra State, Mumbai as a SKMA Nodal Officer. The Tranport Commissioner has also requsted to communicate the appointment of the Nodal Officer to the Nodal officer, Central Key Generation Authority (CKGA), National Informatics Centre, " A " Block, CGO Complex, New delhi-110 003 .

4. Now, vide this Governament Resolution, the sanction is accorded to establish "State Key Management Authority" and to appoint "Deputy Transport Commissioner (Computer), Office of the Commissioner of Transport, Maharashtra State, Bandra (East), Mumbai- 400 051", as the SKMA Nodal Officer. The sanction is also accorded to appoint the another SKMA Nodal Officer to help him and to look after the work of the

..3..

first SKMA Nodal Officer in his absence. The role and responsibilities of the SKMA have been shown in the appendix "A" attached herewith.

5. Similarly, Regional Transport Officers and Deputy Regional Transport Officers wherever the post of Regional Transport Officer does not exist are nominated to work as the RKMA. They would be associated by seniormost Deputy Regional Transport Officers or Assistant Regional Transport Officers as the case may be. The role and responsibilities of RKMA have been shown in Annexure 'B'.

6. The concerned Officers working as SKMA, RKMA and Sub RKMA will be fully responsible to carry out their duties and will be liable for stringent action for their failure to obey the guidelines issued from time to time. The Commissioner of Transport is authorised to communicate the names of the SKMA, RKMA and Sub RKMA Nodal Officers to the "Central Key Generation Authority (CKGA)".

By order and in the name of the Governer of Maharashtra,

(Ramesh Shinde)
Deputy Secretary to the Govt. of Maharashtra,
Home department.

. . . . .

To :

The Commissioner of Transport, Maharashtra State, Mumbai.
Secretary (Information Technology), General Administration Department, Mantralaya , Mumbai-400 032.
Deputy Transport Commissioner (Computer), Maharashtra State, Mumbai.
Shri. S.K. Sinha, Technical Director, Government of India, Ministry of Communications and Information Technology, Department of Information Technology, National Informatics Centre, "A" Block, CGO Complex, Lodhi Road, New Delhi-110003.
All RTO's/ Deputy RTO's
Section Officer's (TRA- 1,2,3, 5), Home Department, Mantralaya, Mumbai.
Select file- TRA-4

Annexure 'A'

Symmetric Key Infrastructure
Roles and Responsibilities

State Key Management Authority

- Authority Card Issuance :- The SKMA nodal officer should access and collate the request received from the RTO's in the state for various classes of master key cards and forward them to the CKGA nodal officer. (Refer Form RTSK1)

- Authority Card Issuance: The SKMA nodal officer should ensure that he receives from the CKGA officer, the same number and types of Authority cards (viz. IA1, IA2, EA and RA etc.) as requested for.

- Authority Card Issuance:- The SKMA nodal officer should collect the Authority cards only after producing a verifiable employee ID card or other satisfactory identity document and furnishing an acknowledgement for the receipt of the Authority cards.

- Authority Card Issuance :-The SKMA nodal officer should send by a courier service/Fax/e-mail his/her confirmation to the CKGA nodal officer about his/her having brought the Authority cards safely to SKMA.

- Authority Card Issuance:- After collecting the Authority cards form the CKGA nodal officer, SKMA nodal officer should be responsible for managing the distribution of the same to different trusted agents in the state.

- Authority Card Issuance:- The SKMA nodal officer should inform the RKMA nodal officer within 1 working day by registered post/Fax/e-mail and ask him/her to collect Authority cards and their respective PIN's from the SKMA.
- Authority Card Issuance:- The SKMA nodal officer should match the acknowledgement along with the signatures received from the RKMA nodal officer with the records.

- Authority Card Issuance :- The SKMA nodal officer should maintain an RTO-wise distribution list for the Authority cards, containing the Authority card details and the details of the RTO/ RKMA nodal officer to whom the Authority cards and PIN's have been issued (Refer Form RTSK3)

- Authority Card Issuance : SKMA Nodal Officer should update the Authority card distribution list every time an RKMA Nodal Officer under it informs of a change of ownership of the Authority card (s) or other particulars of the existing Authority card (s).

- Security Audit : The SKMA nodal officer should ensure that an annual independent security audit of the physical and IT infrastructure of each RTO

within its jurisdiction to the extent used for the issuance of DL cards. location of SKMA system and safe keeping of the Authority cards, is carried out by a technical audit team deputed by NIC, initially and later by a responsible and reputed third party.

- Security Audit :- In addition to the above,t he SKMA nodal officer should also visit the respective RTO from time to time, to inspect and ensure that the DL/RC card issuance process, Authority card management procedures and the database management procedures are being strictly followed.

- Safe Storage: The SKMA Nodal Officer should store the active and backup SKMA cards and their PIN's in a Thick Steel Safe having two lockers and in a manner such that:

Locker 1 has,
- the active SKMA card,
- PIN for the backup SKMA card and,

Locker 2 has,
backup SKMA Card.

- Physical keys to the lockers : As mentioned above, each of the two lockers/ locker chambers will require a pair of keys to unlock. One key from every pair of keys should be in the custody of the SKMA nodal officer. The other key should be in the custody of another officer to be designated by SKMA Nodal Officer.

- Safe Storage : The SKMA nodal officer should be physically present every time the two safes housing the backup SKMA card and its PIN are accessed.

- Usage Counter : The SKMA nodal officer should reset the issuer Authority Cards (DLIA1, DLIA2, RCIA1 and RCIA2) usage counter within 1 working day after receiving request from the RTO nodal officer.

- Master Key Compromise: On receiving request from the RKMA Nodal Officer for arranging the generation of another set of backup Authority cards within the period of 5 working days after being informed about Authority card compromise, the SKMA nodal officer should forward the request to the CKGA nodal officer.

- Master Key Compromise: The SKMA nodal officer should maintain an issuing authority-wise list of damaged/lost/compromised Authority cards, which he would update every time a Authority card damage/compromise is reported by any of the issuing authority.

- Master Key Destruction: The SKMA Nodal Officer should ensure that the compromised, damaged, faulty, Authority card are destroyed-physically and logically- in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key.

- Master Key Destruction : The SKMA nodal officer should be responsible for logging the Authority card destruction activities, including the number and serial numbers of Authority cards, the date and time, names and designations of trusted agents/officials present. The above log should be securely archived for a period of not less than 5 years.

- Master Key Destruction : The SKMA nodal officer should also inform the CKGA nodal officer about the destruction of the Authority cards along with the details.

- The SKMA Nodal Officer shall be responsible for managing the distribution of the PIN's of the Authority cards to the RKMA Nodal Officers in the state only after the SKMA nodal officer has handed over the Authority cards to them.

- AT the time of initial establishment of the Symmetric Key Infrastructure, concerned State Government should appoint/designate the SKMA nodal officer for the state and send by registered post, the SKMA nodal officer's name, and designation and identification details to the CKGA Nodal Officer.

- On being informed of the SKMA key card compromise, the SKMA Nodal Officer should ascertain that the SKMA card has actually been compromised before authorizing and approving the recovery of the backup SKMA Master Key card.

Annexure 'B'

RTO Key Management Authority

- Each RTO shall have a designated RTO Key Management Authority (RKMA) nodal officer and his name, designation and identification details shall be communicated to SKMA Nodal Officer by the RTO.

- The RKMA nodal officer should be responsible for appointing minimum two trusted agents/officials-Issuing Authorities (IA) each for issuance of DL and RC cards.
- The RKMA nodal officer record the name, designation, signature and photograph and other details of all IA's/EA's/RA's and other trusted agents within the jurisdiction of the RTO.

- Authority Card Issuance: The RKMA nodal officer should send the request for required number and Type of Authority Cards to SKMA Nodal Officer (Refer Form RTSK2).

- Safe Storage: The RKMA nodal officer should be responsible for safe storage of the active and backup IA, RA and EA cards in a Thick Steel Safe having Three lockers and in a manner such that:

Safe 1 has,
  - Active IA1 cards,
  - Initial PIN for active IA2 cards,
  - Backup IA2 cards,
  - PIN's for backup RA cards,

Safe 2 has
  - Active IA2 cards.
  - Initial PIN for active IA1 cards,
  - Backup IA1 cards,
  - PIN's for backup EA cards. and

Safe 3 has,
  - PIN's of the back up of IA1 and IA2 cards and.
  - Backup EA cards,
  - Backup RA cards,

- Safe Storage: Active IA1, IA2 cards must be stored in these safes as per the procedure mentioned above at the end of each working day and taken out at the start of next working day.

- Safe Storage: IA1 and IA2 cards should never be kept out of the safe, whenever they are not in use.

- Physical keys to the safe: For the three safes mentioned above, each of the three safe/sage chambers will require a pair of keys to unlock. One key from every pair of keys should be in the custody of the RKMA nodal officer. The other key should be in the custody of the issuing authority.

- Security Audit: The RTO nodal officer should ensure that the KMS software. made available by NIC on behalf of Ministry of Road Transport and Highways, Government of India is used for all DL related activities at the RTO.

- Master Key Issuance: The RKMA nodal officer should collect the Authority cards form SKMA nodal officer by producing a valid employee Id.

- Master Key Issuance: The RKMA nodal officer should also collect the PIN's for the Authority cards from SKMA Nodal Officer by producing a valid employee Id.

- Master Key Issuance : The RKMA nodal officer should furnish an acknowledgement for the receipt of Authority cards and PIN's to the SKMA nodal officer.

- Master Key Issuance: It is the responsibility of the RKMA nodal officer to manage the distribution of the master key cards to the IA's/EA's and RA's in the RTO region. He should inform the IA/EA and RA officials to collect their respective master key cards by registered post within one working day.

- Master Key Issuance: The RKMA nodal officer should ensure that IA's/ EA's/ RA's change their initial PIN's immediately after receiving their Authority cards.

- Master Key Issuance: The RKMA nodal officer should receive an acknowledgement from the IA's/EA's/RA's after issuing them the master key cards and their initial PIN's.

- Master Key Issuance: The RKMA nodal officer should be responsible for ensuring that two IA's(who will issue DL/RC cards in tandem) are provided with IA Authority cards which is a unique pair.

- Master Key Issuance: The RKMA nodal officer , after duly recording the Authority card owner details, should send the acknowledgement back to the SKMA office where the acknowledgement number and other particulars pertaining to the Authority card owner should be recorded by SKMA Nodal Officer.

- Backup : The RKMA nodal officer should be physically present every time the three safes housing the IA, EA and RA and their backup master key cards and their PIN's are accessed.

- Usage Counter : The RKMA nodal officer should forward the request for resetting of IA usage counter received from the two IA's to SKMA Nodal Officer.

- PIN Management : The RKMA nodal officer should ensure that in the event of suspected PIN compromise, new PIN's are generated by all IA's/EA's/RA's for their respective master key cards in the presence of the RKMA Nodal Officer.

- Master Key Compromise: The RKMA Nodal Officer should be responsible for accessing the backup EA and RA Master Key Cards along with their PIN's from the secure safes. These should be handed over to EA/RA only after the receipt of a 'Backup Key Acknowledgement' form duly signed by the EA/RA. The said form should be archived for future records for a period of not less than, when the next audit is conducted.

- Master Key Recovery: The RKMA Nodal Officer should request the SKMA nodal officer to arrange for generation of another set of backup master keys cards within the expiry of 5 working days after being informed about master key card damage/ loss// compromise.

- Master Key Destruction: The RKMA nodal officer should be responsible to ensure that all damaged Authority cards are returned under sealed cover to the SKMA nodal officer. This should also be included by a "Card destruction Request" which should clearly state the number and class of master key cards to be destroyed and the names and designations of officers who were the custodians of the said cards.

- Master Key Destruction: The RKMA nodal officer along with the IA's should be responsible for securely destroying-physically and logically-the damaged, redundant DL/RC cards as per requirement, in a manner that key reconstruction is rendered impossible.

- Master Key Destruction: The RKMA nodal officer should be responsible for maintaining the smart card destruction log, containing details like the number of DL/RC's their serial number, names and designations of the IA's/nodal officer present. This log should be securely archived until the technical audit takes place.

- In case of unavailability of either of the I A's ,the RKMA nodal officer should immediately take possession of the key to the secure safe of that IA. He/she should designate a new trusted official/agent as the new user of the IA card and hand over the keys of the secure safe containing the IA card to him/her with instructions to change the PIN for the IA card immediately.

- IA Card Issuance : the IA should furnish an acknowledgement on receipt of the master key cards and their PIN's to the RKMA nodal officer.

- Key Security: The two IA's should not carry their respective IA cards outside the office premises and securely store them in two separate secure safes inside the RKMA after the working hours.

- Safe Storage: The IA's should ensure that the DL/RC cards after being generated are housed in either of the secure safes used for storing the active set of IA cards.

- Usage Counter : Both the IA's should send a requested, in writing, to RKMA to arrange for replenishment of the usage counter.

- PIN Management: The two IA's should not disclose the PIN's of their IA cards to anybody within or outside RTO. Even the two IA's should not share their PIN information with each other.

- DL/RC Issuance: It is the responsibility of both the IA's to be present at the time of DL/RC key generation. They should ensure that all the keys for the DL/RC card are generated and stored in the DL/RC card such that the DL/RC card is completely functional.

- DL/RC Issuance: The IA's should be responsible for verifying, physically and with the RTO database, the correctness of applicant information in the DL/RCcard, after receiving the printed card from the card personalizer.

- DL/RC Issuance: It should be the responsibility of the IA's to securely archive the DL/RC acknowledgement forms received from the DL/RC distributing officer for a period of not less than 5 years.

- It is the responsibility of each IA to immediately inform the RKMA nodal officer in case of their unavailability / incapacity to perform his/her duties.

- Key Compromise: If the IA believes there has been a compromise of / damage to his/her Authority card, he must promptly notify the RKMA nodal officer.

- Key Compromise: The IA should send a request, in writing, to the RKMA nodal officer to access the backup master key cards and their PIN's in an event of loss/damage/compromise of the master cards.

- DL/RC Destruction: In case of damage of / modification to the DL / RC card, the IA should be responsible for completely destroying the received DL/RC by inboking the 'Comprehensive DL/RC Card Destruction' procedure.

- DL/RC Destruction : The IA's along with the RKMA nodal officer should be responsible for securely destroying-physically and logically-the damaged/ useless DL/RC cards once a week, in a manner that key reconstruction is rendered impossible.

Annexure V

FORMAT OF REQUISITION FORM FOR AUTHORITY CARDS
From RTO to SKMA
(From PTSK2)

Request From.....(RTO Ooffice) Request No..... Request Date.....

Sl.No.	Card Type*	No. of Cards/ Pairs Required* *
1	DL-IA	
2	DL-EA	
3	RC-IA	
4	RC-EA	
5		

(Table-1)

* Card Type : DL-IA, DL-EA, DL-RA,RC-IA,RC-EA, RC-RA,RC-RTO,RC-TC, RC-FI,,RC-IC or RC-PUCC.
** No. of pairs in case of IA & No. of cards in all other cases

Card Holder Information for each cartd is to be furnished in the following formats as the case may be :

1) For IA Cards

There will be two rows corresponding to each IA card mentioned in Table (1). For example, if the r equest is for two DL-IA cards and one RC-IA card then the table will be in thefollowing format.

Sr.No.	Pair No.	IA/IA2	Authority Name	Authority ID	Active (Y/N)	Usage Counter	Office code
1	1	DL-IA1					
		DL-IA2					
1	2	DL-IA1					
		DL-IA2					
3	1	DL-IA1					
		DL-IA2					

2) Forcards otherthan IA Cards

There will be one row corresponding to each non-IA card ,emtopmed om Table (1). For example, if the requestisfor two DL-EA cardsand one RC-EAcard then,thetable will be in thefollowing format.

Sl.No.*	Card No.	Authority Name	Authority ID	Active Y/N	Usage counter	Office code
2	1					
2	2					
4	1					
	2					

Notes:

* Sl.No. - Serial Number as in Table-1.

** Usage counter is the maximum numberof times a card can be used for a particular operation. Forexample, if the usage counterfor a DL-IA card is 100, it means that at the most 100 DL cards can be issued using this pair of IA cards. There is no usage counter in case of EA/RA cards for DL and RC.

Signature
Name &
Designation
(Of the Regional
Key Authority)

Abbreviations used:

DL-Driving License
SKMA-State Key Management Authority
RA-Reviewing Authority
FI-Fitness Inspector
RC-Registration Certificate
IA-Issuing Authority
RTO-Regional Transport Officer
IC-Insurance company.
EA-Endorsing Authority
TC-Tax Collecting authority
PUCC-Pollution under contral Certificate

(Form RTSK 1)

Request for Authority Cards from SKMA to CKGA

State/U.T. MAHARASHTRA STATE Letter No.

Request No. 01/2005 Dated

Authority Card Type	Tick	No. of Cards/Pairs Required*
DL-SKMA		1 CARD
DL-1A		4 PAIRS
DL-EA		4 CARDS
DL-RA		4 CARDS

NODAL OFFICER
STATE KEY MANAGEMENT AUTHORITY.
GOVERNMENT OF MAHARASHTRA

Abbreviations used:

CKGA- Central Key Generating Authority
DL-Driving License
SKMA-State Key Management Authority
EA-Endorsing Authority
STA-State Transport Authority
TC-Tax Collecting Authority
FI-Fitness Inspection
PUCC-Pollution under control Certificate
RC-Registration Certificate
IA-Issuing Authority
RA-Reviewing Authority
RTO-Regional Transport Officer
AU - Authorization authority
IC-Insurance company.